15th ICCRTS "The Evolution of C2"

Integrating Cellular Handset Capabilities with Military Wireless Communications

Topic 1: Concepts, Theory, and Policy
Topic 7: C2 Approaches and Organization
Topic 9: C2 Architectures and Technologies

Captain Joshua Dixon [GRADUATE STUDENT]
(1.75 Yrs completed)
Naval Postgraduate School
1 University Circle, Monterey, CA 93944
831-656-2908
jsdixon@nps.edu

Traditionally, for tactical Command & Control (C2), the Marine Corps utilized strictly voice communications asa result of continued reliability, modern innovative technology vulnerabilities, and the lack of ubiquitous data connectivity. Recently, driven by the technology advances there has been a shift in the paradigm toward more utilization of data applications, such as tactical chat and Blue Force tracker. In this paper, we present distributed, wireless, cellular-handset integration concepts to significantly increase data capabilities on the battlefield. We envision three different technical approaches to integrating cellular handset (i) modifying the handset's software to facilitate tethering with deployed tactical radios, (ii) bridging with a standalone mobile cellular base station, and (iii) modifying the military tactical radios and minimally modifying the cellular handsets to create secure wireless interoperability. An alternative to these solutions would be to entirely replace military communications with a commercial equivalence. In this approach, a mobile base station would provide coverage for each area of operation with a satellite connection for reach back. We analyze each approach regarding its impact on the amount of equipment, reliability or security, and cost per unit. We conclude, based on lab experiments and field testing that the most promising solution is a software upgrade for the commercial cellular handsets and tactical radios to prevent additional hardware dependencies, increase cellular security, and reduce the changes to the current infrastructure.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Integrating Cellular Handset Capabilities with Military Wireless Communications	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Computer Science Department,1 University Circle,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Proceedings of the 15th International Command and Control Research and Technology Symposium (ICCRTS '10), Santa Monica, CA, June 22-24, 2010

14. ABSTRACT

Traditionally, for tactical Command & Control (C2), the Marine Corps utilized strictly voice communications as a result of continued reliability, modern innovative technology vulnerabilities, and the lack of ubiquitous data connectivity. Recently, driven by the technology advances there has been a shift in the paradigm toward more utilization of data applications such as tactical chat and Blue Force tracker. In this paper we present distributed, wireless, cellular-handset integration concepts to significantly increase data capabilities on the battlefield. We envision three different technical approaches to integrating cellular handset (i) modifying the handset?s software to facilitate tethering with deployed tactical radios, (ii) bridging with a standalone mobile cellular base station, and (iii) modifying the military tactical radios and minimally modifying the cellular handsets to create secure wireless interoperability. An alternative to these solutions would be to entirely replace military communications with a commercial equivalence. In this approach, a mobile base station would provide coverage for each area of operation with a satellite connection for reachback. We analyze each approach regarding its impact on the amount of equipment reliability or security, and cost per unit. We conclude, based on lab experiments and field testing that the most promising solution is a software upgrade for the commercial cellular handsets and tactical radios to prevent additional hardware dependencies increase cellular security, and reduce the changes to the current infrastructure.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**9**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Integrating Cellular Handset Capabilities with Military Wireless Communications

Joshua Dixon
Computer Science Department
Naval Postgraduate School
Monterey, CA 93943
jsdixon@nps.edu

Geoffrey G. Xie
Computer Science Department
Naval Postgraduate School
Monterey, CA 93943
xie@nps.edu

Frank Kragh
ECE Department
Naval Postgraduate School
Monterey, CA 93943
fekragh@nps.edu

***Abstract* – Traditionally, for tactical Command & Control (C2), the Marine Corps utilized strictly voice communications as a result of continued reliability, modern innovative technology vulnerabilities, and the lack of ubiquitous data connectivity. Recently, driven by the technology advances there has been a shift in the paradigm toward more utilization of data applications, such as tactical chat and Blue Force tracker. In this paper, we present distributed, wireless, cellular-handset integration concepts to significantly increase data capabilities on the battlefield. We envision three different technical approaches to integrating cellular handset (i) modifying the handset's software to facilitate tethering with deployed tactical radios, (ii) bridging with a standalone mobile cellular base station, and (iii) modifying the military tactical radios and minimally modifying the cellular handsets to create secure wireless interoperability. An alternative to these solutions would be to entirely replace military communications with a commercial equivalence. In this approach, a mobile base station would provide coverage for each area of operation with a satellite connection for reachback. We analyze each approach regarding its impact on the amount of equipment, reliability or security, and cost per unit. We conclude, based on lab experiments and field testing that the most promising solution is a software upgrade for the commercial cellular handsets and tactical radios to prevent additional hardware dependencies, increase cellular security, and reduce the changes to the current infrastructure.**

I. INTRODUCTION

This paper focuses on military communication assets normally inherent to Marine Corps Infantry company level elements, because of the first author's familiarity with the technology and needs of the warfighter. However, the concepts explained throughout the paper can be applied independent of any one service. Current communications inherent to the company level consist of single channel, half duplex radios. These radios are becoming increasingly more capable with the ability to transfer data across the same link as for voice. Recent technological advances in tactical radios facilitate the capability of sending and receiving standard Internet Protocol (IP) packets. This characteristic increases the capability of the radios to support the requirements of network-centric, modern warfare. As Marine Corps General Alfred M. Gray said to Congress in the 90's, "Intelligence without communications is irrelevant, communications without intelligence is noise." Timely intelligence dissemination is extremely critical in modern warfare. The traditional method of transmitting intelligence solely via voice communications fails to provide efficient results. For example, the saying, "a picture is worth a thousand words," seems accurate when attempting to describe a suspect's physical description. It might take a soldier a couple of minutes to transcribe or explain the description; however, a picture captured through a cellular handset or digital camera could drastically increase the accuracy of information, while reducing message generation times. Every warfighter is capable of collecting intelligence; however, until recently only radio operators were capable of disseminating this information via a voice transmission. This paper will discuss various methods to further extend the IP based capability out to every ground troop. The concept facilitates the idea of providing every Sailor, Soldier, Marine, and Airmen the ability to send and receive communications from a handheld device, while in garrison or operationally deployed. This revolutionary technology which excelled the commercial sector light years ahead can now advance our battlefield communication infrastructure without crippling the integrity.

II. PROBLEM

Modern cellular handsets lead a wave of innovations within the commercial industry to provide revolutionary business capabilities, but are nonexistent in military operational environments. This is in part due to the security vulnerabilities of the current commercial cellular technology. Yet such devices bring many capabilities of a traditional personal computer in a handheld form factor and at an extremely low cost in comparison. It is unwise to totally ignore their potential for delivering information across the battlefield at high capacity data rates. The Marine Corps attempted to leverage a similar commercial technology by adopting the components of a personal digital assistant (PDA) and converting it into a Dismounted Data Automated Communication Terminal (D-DACT) to meet military specifications. However, the end result increased the cost from roughly a $400 Commercial-Off-The-Shelf (COTS)

PDA to a $10000 - $15000 Government-Off-The-Shelf (GOTS) device. The size increased from a couple ounces to a couple pounds with batteries attached. The tradeoff in size and price significantly limit the desirability of the technology. Future integration attempts must maximize the commercial technology while limiting changes necessitated by mitigating essential security vulnerabilities.

The primary function of the D-DACT devices is for situation awareness enhancement. Obviously, these devices are extremely useful as opposed to a standard map and compass. They are a valuable asset for the specific individuals assigned as navigators; however, the remaining troops lack additional communication capabilities beyond their handheld, voice-only radios. The radios capable of transmitting data are traditionally assigned to select individuals; although, the radio's data capability can only be leveraged if tethered to a PC via a dongle and Ethernet cable making their use unsuitable for dismounted soldiers. Therefore, at least at the company level, we routinely fought in voice-only communications environment.

A. Centralized Architecture

The most capable integrated voice and data device capable of extending the military's tactical edge without further encumbering the user seems to be cellular handsets. However, traditional cellular architectures depend on highly reliable, land-based networks. Multiple base stations coordinate and exchange traffic via switching centers, imposing a centralized, hierarchical architecture. This is problematic for environments that require a highly-mobile, ad-hoc, wireless network. In an intermittent communications environment the centralized architectures fail to meet the common criteria of providing independency. Additionally, centralized architectures can create single points of failures with the potential for catastrophe: if one link dies, the entire communication tree structure fails below the severed connection.

B. Hardware Security

As specified by the National Institute of Standards and Technology (NIST) military radios capable of holding Communication Security (COMSEC) cryptographic material needs to comply with Federal Information Processing Standards (FIPS) 140-2 level 2 or higher in order to prevent tampering or reverse engineering of cryptographic devices [1]. This capability is not inherent to commercial cellular handsets. To achieve these requirements, significant modifications are required of the electronic components. As these modifications require hardware changes, the potential for individual unit cost significantly increases. In addition to high cost, these hardware modifications would require additional COMSEC procedure considerations. As with current COMSEC devices that require special handling, accountability, and storage restrictions, these modifications would inhibit convenience and reduce desirability.

C. Information Security

The same standard, FIPS 140-2, designed to protect cryptographic devices, alludes to the level of encryption required for each security classification. However, High Assurance Internet Protocol Encryptor (HAIPE) or Suite B are National Security Agency (NSA) categories specifically designed to aid in the creation of devices or algorithms for protection of classified information [2,3]. Commercial industry does manufacture a HAIPE categorized cell phone (Secure Mobile Environment Portable Electronic Device (SME PED)) [4]. These are Type 1 NSA approved devices for transmitting classified data across the cellular networks. The disadvantages to this device are the relatively high cost, single vendor market, and lack of software portability. Alternatively, the Suite B category was created to enable non-hardware specific development (software algorithms) for commercial products to process classified information. This facilitates decoupling the hardware from the encryption process. Accordingly, a software algorithm (e.g. AES 256) can protect data with up to a SECRET classification. This is advantageous for commercial cellular handsets vendors because many devices are capable of performing software encryption and decryption at suitable speeds.

D. Emission Security

Even if commercial cellular handsets were generic enough to eliminate the desire for reverse engineering or contained encryption algorithms suited for protecting information at an appropriate classified level, the devices are still insufficient for "outside-the-wire" operations. Low Probability of Detection (LPD) signals are the "result of measures used to hide or disguise intentional electromagnetic transmissions [2]." These types of signals delay or prevent an adversary from determining if the signals exist [5]. Low Probability of Intercept (LPI) signals are "the result of measures to prevent the intercept of intentional electromagnetic transmissions [2]." This type of signal either delays or prevents an adversary from capturing the detected signal [5]. Spread spectrum signals have potential to mitigate vulnerabilities by spreading the signal across a wide-band when the adversaries are without the synchronization schemes [5]. However, although Code Division Multiple Access (CDMA) signals leverage spread spectrum, the synchronization schemes for cellular standards remain in the public domain to allow interoperability. Furthermore, the spread-

ing in these cellular standards is insufficient for adequately reducing the magnitude of the signal's power spectral density to be considered LPD or LPI at reasonable distances. Therefore, the spread spectrum characteristic will not solely provide enough protection against the potential threat without a private, custom spreading scheme.

III. Related Work

There exist numerous exercises and events aimed at integrating cellular technology with military communications [6] [7]. However, the topologies normally leverage satellite connectivity for reachback communications, which is rarely readily accessible by the majority of combat units. From the personal experience of the first author, only high priority missions or division level units are allocated satellite channels. Additionally, each exercise is developed as a demonstration of industry's innovative technologies with dozens of vendor consortiums. However, the concepts are designed for higher level, large scale employments. These implementations all fail when applied to a company and below level element. The primary takeaways from these demonstrations are the growing importance of voice over internet protocol (VoIP) infrastructures and the requirement of various switches to integrate legacy communication equipment. These characteristics are common and necessary for any scalable communication architecture.

In our research we have found a couple of industry leaders have available units to demonstrate a true Peer-to-Peer (P2P) architecture where traditional cellular base stations are no longer a requirement. These phones are capable of forming an internal ad-hoc wireless network without any access point dependencies. However, as the technology is just developing the cost per unit outweighs the benefit of the technology.

The Joint Program Executive Office (JPEO), Joint Tactical Radio Systems (JTRSs) has developed the Software Communication Architecture (SCA) and Application Programming Interfaces (APIs) standards to facilitate interoperability between military communication assets [8]. The intent is to build software with Government Purpose Rights (GPR) capable of leveraging the Software Define Radio (SDR) characteristics in an effort to facilitate innovative technologies and allowing future integration. For example, a JTRS waveform named the Mobile User Objective System (MUOS) Common Air Interface (CAI) is capable of providing Military Satellite Communications (MILSATCOM). This waveform was developed from a cellular protocol (i.e., wideband CDMA (WCDMA)) [9]. The relevant work associated with the effort is the open architecture concept with cellular air interface. This provides a framework or platform to implementing our concepts without hardware modifications.

The idea of leveraging cellular technology is desirable for many reasons, however, without GPR the concepts receives little attention. A second generation (2G) cellular open source base station (OpenBTS) project was initiated to bring the cellular technology to the developing world at a fraction of the cost. Their work is related, because they decouple the GSM air interface from the remaining switching requirements traditional to the protocol. The entire software based base station code operates on a Linux OS with an attached RF frontend provided by a SDR.

Since the traditional fixed cellular infrastructure is not suitable for employment in highly-mobile, military operations, nor responsive enough for disaster response and relief activities, commercial industry has developed mobile variants. These mobile variants normally contain the infrastructure of the cellular technology in two man portable containers. The intent of the design is for the devices to be deployed aboard an aerial platform, land vehicle, or at a remote Forward Operating Base (FOB). The devices are capable of providing 2.5G/3G/4G cellular service. The coverage areas of these devices are dependent on the technology and the terrain throughout the Area of Operations (AO). The technology has been demonstrated at various military exercises; however, to our knowledge no U.S. military service has deployed any of the devices in an operational capacity [6] [7] [10]. These devices employ the same type of signals resident within traditional cellular base stations. The main advantage to the form factor is the mobility characteristic. Since these devices are man-portable and vehicle-mountable, the technology can support highly mobile operations. In addition to the form factor and with added software or hardware, the Mobile Base Stations (MBS) can be supplemented with end-to-end or link encryption algorithms for protecting the data. However, given the COTS technology, the signals lack the Emission Control (EMCON) requirements of typical military applications.

IV. Concepts

The following concepts were determined to be the most feasible. However, they are not a comprehensive representation of the possibilities.

A. Bridging Device Concept

As mentioned in the related work section, the commercial industry attempts to mitigate the vulnerabilities associated with intermittent backhaul communications (i.e. the centralized

architecture vulnerability) by reducing the hardware footprint to self-contained, mobile modules. These devices were designed to support large numbers of users and come with an extremely high per unit cost. Further, the concept of employment needs to take into consideration down time for equipment failures; otherwise, the large number of supported users could potentially remain without communications. Based on these considerations and emission security vulnerabilities the bridging concept should only be considered for garrison or "inside the wire" employment scenarios. This bridging concept facilitates integrating a completely unmodified COTS technology, essentially creating a cost effective solution. However, considering the wireless vulnerabilities any outside-the-wire operations are not feasible with high EMCON level restrictions.

B. Tethered Concept

In order to integrate the technology without delaying years for the acquisition process and DoD policy changes, a tethered approach can provide the interim solution. This concept requires software modification to a preexisting ruggedized cellular handset. The software modification enables the handset to directly connect to a tactical radio via a shared USB to Ethernet cable. Currently traditional handsets are configured as USB clients for data transfers. This concept modifies the software by adding the USB host functionality. In the end, allowing the handset to attach as an additional network node from any IP capable radio. As before, end-to-end encryption algorithms are desirable for content protection. The disadvantage to this concept is fairly evident given the wired connection between the device and the tactical radio.

C. Directly Via Wireless Interface Concept

In order to eliminate the proximity limitation a wireless interface is required. The final concept assumes the tactical radios can provide a platoon size element sufficient communication capabilities when integrated with cellular handset interoperability. This concept modifies the military radios to act as access points when beyond either commercial cellular connectivity or inherent mobile base stations range (i.e. the first concept). We suggest five major modifications to the handset and tactical radio: (i) limited handset modifications, (ii) leverage Software Defined Radio (SDR) characteristics inherent to tactical radios, (iii) LPI modification to the cellular air interface, (iv) decoupling the air interface from remaining infrastructure requirements, and (v) including client software for sufficient content protection.

1. Strategic Modifications Based On Cost

In an effort to minimize cost, while increasing integration feasibility the majority of the modifications shall reside on the tactical radios vice the handsets. The proposed modifications to the cellular handsets shall be limited, because the potential demand will never significantly offset production cost. Given the tactical radios are already extremely expensive in comparison the leveraged tactical radio platform shall contain hardware characteristics capable of integrating the technology via software modifications. For example, the MOUS waveform leverages the Wideband-CDMA protocol, which in comparison to our single channel half duplex radios could minimize additional hardware requirements.

2. Software Defined Radio Characteristic

This concept suggests leveraging modern tactical radios containing Software Defined Radio (SDR) functionality with the Radio Frequency (RF) frontend (i.e. two transceivers) capable of hosting the chosen cellular waveform. By leveraging these SDR characteristics inherent to our upcoming company level radios the concepts becomes feasible through a firmware upgrade eliminating potential hardware modifications. This modification reduces the overall cost of employment and eliminates the dependency on single vendor solutions, however, fails to account for emission security vulnerabilities.

3. Air Interface Consideration

As mentioned before, the overall cost greatly affects the level of feasibility. In effort to minimize cost thus minimizing handset modifications a cellular air interface should be leveraged and modified to incorporate LPI characteristics. A commercial cellular air interface is suggested vice the military equivalent, because the handset's residual hardware (i.e. the RF frontend, etc.) only support cellular protocols. Otherwise, the handsets hardware would need completely redesigned. As mentioned previously, the modification to the tactical radios to support this interface is minimal on radios containing the MUOS waveform. The IEEE 802.16e standard contains desirable functionality, but is still vulnerable to various attacks. Therefore, if the protocol is modified to mitigate these limitations the remaining hardware would support the new chipset. In this example, the tactical radios would need to be modified to incorporate the new 802.16e standard. When developing this new air interface specific frequency allocation considerations should be taken to account for the potential environments military services will encounter. An example of this concept is the Harris SecNet 11 technology. SecNet 11 was developed from the 802.11 standard and provides Type-1 security [11].

4. Interoperability Consideration

In an effort to eliminate the traditional centralized cellular architecture and increase interoperability with legacy systems, a decoupled air interface is required to eliminate remaining infrastructure dependencies. For example, the air interface can provide sufficient connectivity from the handsets to the tactical radios and a secure Voice over Internet Protocol (VoIP) infrastructure can provide backhaul interoperability. This would require the tactical radios to host a private branch exchange server for routing local calls in addition to integrating larger systems. For data, the radio would consolidate the frames into packets and route accordingly. However, the content is not protected without some level of encryption within each layer.

5. Content Protection Consideration

When considering protecting the data each device will need the ability to authenticate, encrypt, and decrypt the information being transmitted. When developing this software solution, a Suite B algorithm is desirable to prevent provisioned handsets from requiring hardware modifications to account for cryptographic interoperability. With a Suite B algorithm, the handsets would not be required to adhere to restrictive COMSEC handling procedures. Obviously, the associated tactical radios need to be retrofitted with the same algorithms. However, this seems less difficult since commercial industry already advertises radios with this capability [12].

V. EXPERIMENTS

The concepts presented in the previous sections require specific testing for validation. As a starting point and based on the current capabilities resident in the commercial market, we recently conducted a series of proof-of-concept experiments. The section is divided into one field environment and two lab exploration experiments.

A. CELLULAR BRIDGE EXPERIMENT

In an effort to explore the feasibility of hosting cellular Local Area Networks (LAN)s at the edge of military tactical Wide Area Networks (WANs), we designed an experiment to leverage commercial cellular mobile base stations as bridging devices. In the process of exploring the feasibility of extending our tactical networks by including cellular edges we designed an integrated architecture and evaluated it during a Tactical Network Topology (TNT) Capabilities Based Experimentation (CBE) exercise. The Naval Postgraduate School conducts the TNT exercises quarterly in Camp Roberts, CA and remote locations.

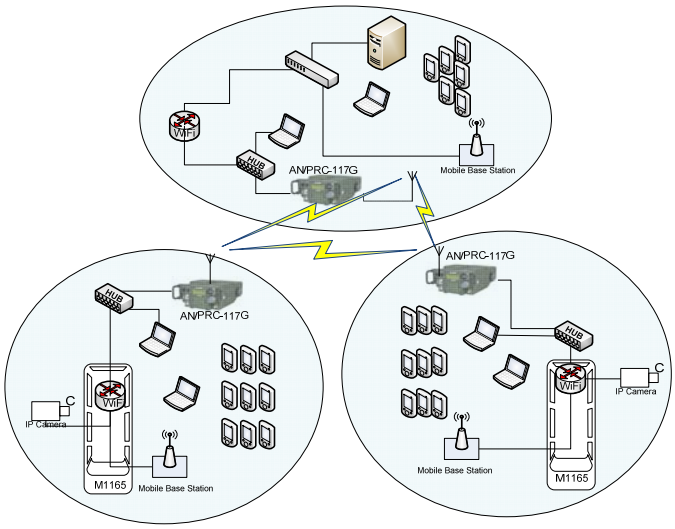

Figure 1 - TNT CBE Topology

Our participation during the TNT event was limited to evaluating the tactical radio throughput restrictions, the throughput of commercial base stations, and the resource requirements needed to support cellular handset integration. The topology (Figure 1) was designed to force each cellular base station to utilize military tactical radio links for interconnectivity. The design includes:

- (3) wirelessly interconnecting Harris AN/PRC-117G radios configured with the Advanced Networking Wideband Waveform (ANW2) to act as one Mobile Ad-hoc Network (MANET).
- (3) tethered LGS Innovation's Tactical Base Station Routers (TacBSRs), which are 2.5G mobile cellular base stations (2 Picocells emitting 320 mW and 1 Marcocell emitting 20W)
- (3) Cisco 3200 Series WiFi Ruggedized Routers (leveraged to benchmark against GPRS throughput)
- (2) vehicle mounted Sony IP Cameras
- (18) Nokia E51s, (3) HTC Touchs, and (3) HP iPAQ Cell Phones
- Dell PowerEdge 2850, 3GB Processor, 8GBs RAM, with Windows 2003 Server & Reality Vision (video software)

The AN/PRC-117G radios are capable of directly connecting via the Ethernet dongle to an external computer or handheld device without intermediate switch or router. However, for this experiment we included additional devices for added functionality. The ANW2 mission plan was configured for 305.00 MHz as the center frequency with 5 Mhz bandwidth. During our throughput testing the radios displayed a Waveform Identification (WID) number of seven. With only a few

tests due to limited time, we observed a wired UDP rate of 250 – 350 Kpbs and a TCP rate of 20 – 25 Kbps leveraging Test TCP (TTCP) as the measurement tool [13]. The tests were not comprehensive, did not take place in multiple environments, and are not intended for evaluating the waveforms potential. However, the results suggest integration feasibility excluding operational employments requiring a high level of emission security. As explained in section II.d., these emission security requirements are unattainable without modifying the cellular signals or introducing a military waveform on a cellular handset. Throughout the exercise, the tactical SDRs successfully hosted two separate Pico-cell and one Macro-cell networks, each containing six simultaneous voice / data channels. Essentially we converted a single channel half-duplex radio into a six-channel full duplex cellular base station access point.

In an effort to evaluate the potential of live video streaming from a mobile platform to either a fix site (i.e. HQ element) or additional mobile platform, we leveraged commercial software (Reality Vision). For this experiment we conducted a series of test benchmarking the GPRS, WiFi, and wired LANs (Figure 2). The wireless streaming video initiated from a cellular handsets internal camera, then traversed either the GPRS or WiFi routers. The fixed IP cameras feed traversed a wired link until crossing the tactical radios. To test the GPRS capability (Figure 2), we disabled the WiFi interface on the handsets. At first, the observed frame rates discredited the concept of leveraging these military radios for streaming live video. However, after disabling the GPRS and enabling the WiFi interface (Figure 3), the observed delay was trivial in comparison. To test the theory we eliminated all wireless cameras by directly connecting fixed IP cameras via the tactical radios Ethernet cable (Figure 4). The observed delays were similar to the WiFi access point delays.

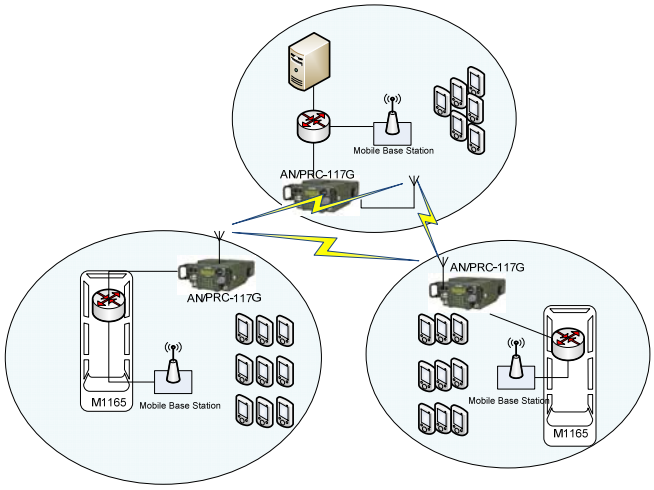

Figure 2 - GPRS Topology

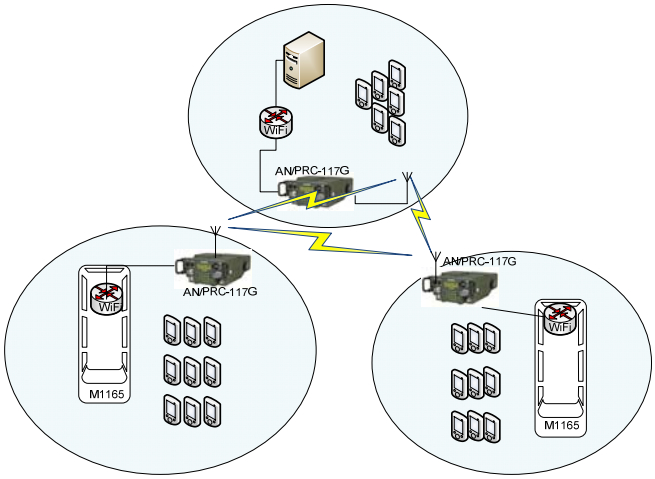

Figure 3 - WiFi Topology

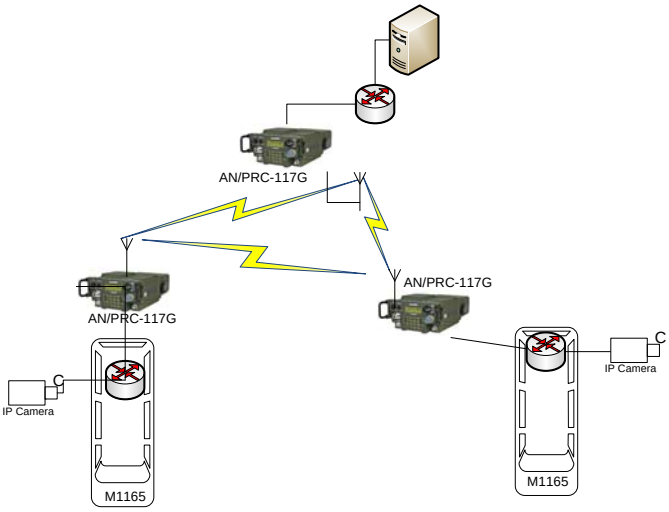

Figure 4 - Fixed IP Camera Topology

We conclude the tactical radios leveraged were not a bottleneck when interconnecting GPRS capable base stations. The results suggest a potential for hosting 3G networks on the edge of our tactical networks [13].

B. Tethered Exploration

For the tethering concept, we carried out some preliminary lab exploration to determine concept validity. We found cell phones can easily connect to an IP based network through a USB cable attached to a personal computer. However, we have been unsuccessful in directly connecting an Ethernet dongle from an IP capable tactical radio. After reviewing a couple of devices (HTC Dream with Android OS, Apple's

iPhone, and RIM's Blackberry) we concluded the hardware is capable of providing the functionality by leveraging a Universal Serial Bus (USB) On The Go (OTG) Host characteristic, but in the absence of a working device driver we cannot indisputably conclude on the feasibility [14] [15].

C. Wireless Interface And Software Defined Radio Exploration

As a step toward solidifying our feasibility assessment of integrating a cellular base station capability via a software implementation, we configured in a lab environment, the open source OpenBTS software on a Linux computer with attached SDR (USRP v1). The OpenBTS software provided the BTS capability, when concurrently run with a few OS (Ubuntu 9.04) inherent programs. The open source VoIP software Asterisk was initiated to account for the Private Branch Exchange (PBX) requirement. GNURadio was installed and initiated as the signal processing package (USRP initiator). A VoIP client was installed to initiate voice calls from the computer. The most relevant hardware difference between our tactical radios and the USRP configuration appears to be the dual transceivers needed for the BTS full-duplex characteristic as most tactical radios have only one transceiver. The results of our lab configurations suggest that for a complete off-the-shelf software integration concept the OpenBTS software is feasible with two tactical radios. However, more testing is needed to determine the level of feasibility. For example, a requirement of two radios to run a vulnerable cellular signal seems improbable when an additional radio is still needed for reachback connectivity. As an alternative, a MUOS capable SDR should be considered since the waveform already shares similar properties with WCDMA [9]. The related work to this project is closely coupled to the Joint Tactical Radio System program. Production radios are not available with the MUOS waveform. Therefore, specific testing beyond these initial observations is not possible.

VI. Conclusion and Future Work

In summary, the concepts mentioned during this paper appear feasible. The tethering concept is an "age old" "tried and true" method, however, the COTS handsets are not developed for military austere environments. Perhaps, given the high demand for a near term solution, the handheld devices are restricted to environments not requiring the complex ruggedized hardware. These phones are currently hundreds of dollars compared to thousands of dollars for each military tactical radio. The concept of buying disposable cell phones ($300 versus $2000) might provide the interim solution and policy suggestion as an alternative to the high priced ruggedized variation. These devices would still be required to pass through the government certification and accreditation process. However, to leverage the innovative technology perhaps minimal risk is acceptable. Our results show the leveraged tactical radios are capable of successfully interconnecting 2.5G cellular base stations. Therefore, we've demonstrated the possibility of connecting commercial innovative cellular handset to our tactical radios via an external bridge device. However, more exploration is required to determine the estimated cost, level of feasibility, and complexity for developing a non-bridged proof of concept. Our research lacked the resources to implement various concepts on relevant FPGAs. The next step beyond our approaches would be to implement the software on an FPGA similar to those contained within military tactical radios. This will require significant modification to the BTS software to account for the different hardware.

VII. Acknowledgements

The authors would like to recognize our supporters (Marine Corps Systems Command, LGS Innovations, Reality Mobile, and the OpenBTS project) for either loaning us equipment, providing valuable resources, or outright funding the effort. In addition, we would like to thank Rob Beverly and John Gibson for their rigorous editing reviews.

VIII. References

[1] Information Technology Laboratory, "Federal Information Processing Standards Publication," National Institute of Standards and Technology, Gaithersburg, Publication 2002.

[2] CNSS Glossary Workign Group, "National Information Assurance (IA) Glossary," CNSS Instruction No. 4009, 2006.

[3] National Security Agency. (2009, December) NSA Suite B Cryptography. [Online]. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[4] General Dynamics. (2009, December) General Dynamics C4 Systems. [Online]. http://www.gdc4s.com/content/detail.cfm?item=32640fd9-0213-4330-a742-55106fbaff32

[5] Richard Poisel, *Modern Communicatoins Jamming Principles and Techniques*. Norwood, USA: Artech House Inc, 2004.

[6] Joint Fires Integration and Interoperability Team, "Tactical Cellular Limited Operational Assessment Report," Unitied States Joint Forces Command, Eglin AFB, LOA TR-09-03, 2009.

[7] Executive Agent for Theater Joint Tactical Networks (EA-TJTN), "Joint User Interoperablity Communications Exercise (JUICE) 2009," Final Report 2009.

[8] Joint Program Executive Office Joint Tactical Radio Systems. (2005, August) JPEO JTRS Overview to OMG. Power Point. [Online]. http://jpeojtrs.mil/

[9] Department of the Navy Research, Development & Acquisition. (2010, January) MUOS Mobile User Objective System. [Online]. https://acquisition.navy.mil/rda/home/programs/information_communications/muos

[10] Joint Systems Integration Center. (2009, Septemeber) Tactical Cellular Presentation. Power Point.

[11] Harris RF Communications. (2009, December) Harris Corporation.

[Online]. http://www.rfcomm.harris.com/products/embeddable-security/

[12] Harris RF Corporation. (2009, December) Tactical Radio Communications. [Online]. http://www.rfcomm.harris.com/products/tactical-radio-communications/RF-310M-HH.pdf

[13] Military Wireless Communications (MWC) Research Group, "Military Wireless Communication (MWC) Group TNT / CBE 10-1 After Action Report," Naval Postgraduate School, Monterey, After Action Report 2009.

[14] Google Inc. (2009, December) Android FAQ. [Online]. http://android-dls.com/wiki/index.php?title=Android_FAQ

[15] Apple Inc. (2009, December) MAC Dev Center: USB Device Interface Guide. [Online]. http://developer.apple.com/mac/library/documentation/DeviceDrivers/Conceptual/USBBook/USBIntro/USBIntro.html

[16] Harris Corporation. (2009, June) AN/PRC-150(C) Advanced Tactical HF Radio Data Sheet. [Online]. www.rfcomm.harris.com

[17] Harris. (2009, September) Harris AN/PRC-152 Type 1 Multiband Multimission Handheld Radio Data Sheet. [Online]. www.harris.com

[18] Harris Corporation. (2009) Harris RF Communications. [Online]. www.rfcomm.harris.com

[19] Thales. (2005, September) Thales Communications. [Online]. www.thalescomminc.com